IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)	:	Kazuo J. EZAWA *et al.*
Serial No.	:	09/628,315
Filed	:	July 28, 2000
For	:	SYSTEM AND METHOD FOR COMMUNICATING BETWEEN SMART CARDS
Examiner	:	Aravind K. Moorthy
Group Art Unit	:	2131

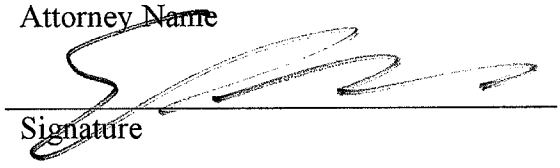
RESPONSE TO ORDER RETURNING UNDOCKETED APPEAL TO THE EXAMINER FROM BPAI

I hereby certify that this paper is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

September 9, 2008
Date of Deposit

Eliot D. Williams
Attorney Name

50,822
PTO Registration No



Signature

September 9, 2008
Date of Signature

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

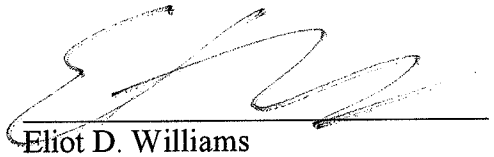
This paper is submitted in response to the Order Returning Undocketed Appeal to the Examiner from BPAI (hereafter "Order"), dated May 15, 2008. The Order states *inter alia* that "on page 2 of the Examiner's Answer, under the heading "Summary of Claimed Subject Matter" the Examiner stated that "The Summary of claimed subject matter contained in the brief is deficient..."",

Order, page 2. Consequently, the BPAI ordered the Examiner to "notify applicants to file a paper providing a summary of the claimed subject matter as required by 37 CFR 41.37 (c)(1)(v)", *Order, page 3.* However, applicants respectfully state that such a summary has been filed by applicants already and can be found on the page 6 of the applicants' Appeal Brief filed on July 23, 2007 and which is enclosed here for the Examiner's convenience.

Accordingly, applicants respectfully disagree with the Examiner's suggestion that the summary of claimed subject matter is deficient and respectfully request the Examiner to reconsider.

If there are any remaining issues to be resolved, applicants respectfully request the Examiner to contact the undersigned attorney by telephone for an interview.

Respectfully submitted,



Eliot D. Williams
Patent Office Reg. No. 50,822

BAKER BOTTS L.L.P.
30 Rockefeller Plaza, 44th floor
New York, New York 10112-0228

Attorney(s) for Applicant(s)
(212) 408-2563

AP32610 - 072817.0152

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

On Appeal to the Board of Appeals and Interferences

Appellant(s)	:	Ezawa et al.	Examiner:	Aravind K. Moorthy
Serial No.	:	09/628,315	Group Art Unit:	2131
Filed	:	July 28, 2000		
Title	:	SYSTEM AND METHOD FOR COMMUNICATING BETWEEN SMART CARDS		

APPEAL BRIEF

I hereby certify that this paper addressed to: Commissioner for Patents, P.O. Box 1450, Arlington, VA 22313-1450 is being via facsimile to the United States Patent and Trademark Office at 571-273-8300 on the date below:

July 23, 2007
Date of Deposit

Manu J Tejwani	37,952
Attorney Name	Registration No.
Signature	July 23, 2007
	Date of Signature

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

A31906-A - 070457.1195

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

On Appeal to the Board of Appeals and Interferences

Appellant(s)	:	Ezawa et al.	Examiner:	Aravind K. Moorthy
Serial No.	:	09/628,315	Group Art Unit:	2131
Filed	:	July 28, 2000		
Title	:	SYSTEM AND METHOD FOR COMMUNICATING BETWEEN SMART CARDS		

APPEAL BRIEF

Commissioner for Patents
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

On May 22, 2007, Appellants filed a Notice of Appeal from the final rejection of more than twice-rejected claims 1-58 contained in the Office Action dated on February 22, 2007. The U.S. Patent and Trademark Office received the Notice of Appeal on February 22, 2007.

Applicants hereby timely submit, pursuant to 37 C.F.R. § 41.37, an Appeal Brief in support of the appeal of the rejection of pending claims 1-58.

I. REAL PARTY IN INTEREST

The real party in interest is MasterCard International Incorporated, 2000 Purchase Street, Purchase, New York 10577-2509 ("MasterCard") by virtue of purchase agreement with MONDEX INTERNATIONAL LIMITED assignee of the entire right, title, and interest in the present application by virtue of the Assignment dated July 25, July 26 and July 27, 2000,which was recorded on October 2, 2000 at Reel 1140 Frame 0006.

II. RELATED APPEALS AND INTERFERENCES

Appellants and the Appellants' legal representatives are unaware of any appeals or interferences related to the present application, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-58 stand rejected under 35 U.S.C. § 112, first paragraph as failing to comply with the written description requirement.

Claims 1-44 and 46-58 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Ishiguro et al. U.S. Patent No. 5,502,765 ("Ishiguro"). Claims 4 and 45 stand rejected under 35 U.S.C. § 103(a) as being obvious form Ishiguro in view of Carlisle et al. U.S. Patent No. 5,649,118 ("Carlisle").

Claims 1-58 are now on appeal.

IV. STATUS OF AMENDMENTS

Appellants have filed no further amendments to the claims subsequent to the issuance of the Final Official Action dated February 22, 2007.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Appellants' invention provides systems and methods for direct but secure transactions between smart cards (or other portable devices) without the need for accessing a host system to verify or authenticate process parameters such as time. According to applicants' invention, each smart card is embedded with its own trusted time clock, reference or parameter. (See e.g., specification page 5, lines 14-20). The embedded trusted time parameter may be hashed or otherwise represented by a sequence of numbers.

Independent claims 1, 25, 32, 37, 41, and 54 are directed to the inventive systems and methods. All of these independent claims 1, 25, 32, 37, 41, and 54 require key-secured communication between two smart cards to mutually update information based upon a comparison of trusted times that are embedded in each of the two smart cards. (See e.g., specification, page 18, lines 19-26.)

Written support for independent claims 1, 25, 32, 37, 41, and 54 may be found in the specification as indicated below:

1. A method for communicating between a first portable device having a first storage device and a second portable device having a second storage device, the first storage device storing thereon a first sequence number and a first key, the second storage device storing thereon a second trusted time and a second key, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices, the method comprising the steps of:

comparing the first sequence number to the second sequence number including comparing the embedded first and second trusted times;

performing a verification using the first and second keys;

if the second sequence number is newer than the first sequence number by comparison of the respective embedded first and second trusted times, setting the first sequence

number to have a value of the second sequence number if the verification succeeds; and conversely,

if the first sequence number is newer than the second sequence number by comparison of the respective embedded first and second trusted times, setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device [*See e.g., specification, page 18, lines 19-26*].

25. A portable device which is capable of performing a transaction with a further portable device, comprising:

a storage device storing a first sequence number and a first key wherein the first sequence number comprises information on a first trusted time embedded in the storage device; and

a processing device performing the following steps:

receiving a second sequence number and a second key from the further portable device, wherein the second sequence number comprises information on a second trusted time embedded in the further portable device,

comparing the first sequence number to the second sequence number including comparing the embedded first and second trusted times;

performing a verification using the first and second keys;

if the second sequence number is newer than the first sequence number by comparison of the respective embedded first and second trusted times, setting the first sequence number to have a value of the second sequence number if the verification succeeds; and conversely,

if the first sequence number is newer than the second sequence number by comparison of the respective embedded first and second trusted times, setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device[*See e.g., specification, page 18, lines 19-26*]..

32. A method for determining an approximate current time using a first portable device and a second portable device, the first portable device having a first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number, the second storage device storing thereon a second sequence number, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices, the method comprising the steps of:

comparing the first sequence number to the second sequence number, the first sequence number being indicative of ~~a~~ the first trusted time provided on the first portable device, the second sequence number being indicative of ~~a~~ the second trusted time provided on the second portable device; and

if the first trusted time is older than the second trusted time, setting the first sequence number to have a value of the second sequence number and conversely,

if the second trusted time is older than the first trusted time, setting the second sequence number to have a value of the first sequence number so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device [*See e.g., specification, page 18, lines 19-26*]..

37. A portable device which is capable of determining an approximate current time during a communication with a further portable device, comprising:

a storage device storing a first sequence number wherein the first sequence number comprises information on a first trusted time embedded in the storage device; and

a processing device performing the following:

receives a second sequence number from the further portable device number wherein the second sequence number comprises information on a second trusted time embedded in the further portable device,

compares the first sequence number to the second sequence number, the first sequence number being indicative of ~~a~~ the first trusted time provided on the

portable device, the second sequence number being indicative of ~~a~~ the second trusted time provided on the further portable device, and

executes one of the following actions:

if the first trusted time is older than the second trusted time, sets the first sequence number to have a value of the second sequence number; and conversely,

if the second trusted time is older than the first trusted time, sets the second sequence number to have a value of the first sequence number so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device [*See e.g., specification, page 18, lines 19-26*]..

41. A method for determining an approximate current time using a first portable device and a second portable device, the first portable device having a first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number and a first key, the second storage device storing thereon a second sequence number and a second key, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices, the method comprising the steps of:

comparing the first sequence number to the second sequence number, the first sequence number being indicative of ~~a~~ the first trusted time provided on the first portable device, the second sequence number being indicative of ~~a~~ the second trusted time provided on the second portable device;

if the second trusted time is newer than the first trusted time, performing a verification using at least one of the first and second keys; and

setting the first sequence number to have a value of the second sequence number if the verification succeeds; and conversely,

if the first trusted time is newer than the second trusted time, performing a verification using at least one of the first and second keys; and

setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device[*See e.g., specification, page 18, lines 19-26*]..

54. A portable device which is capable of determining an approximate current time during a communication with a further portable device, comprising:

a storage device storing a first sequence number and a first key wherein the first sequence number comprises information on a first trusted time embedded in the storage device; and

a processing device performing the following:

receives a second sequence number and a second key from the further portable device wherein the second sequence number comprises information on a second trusted time embedded in the further portable device,

compares the first sequence number to the second sequence number, the first sequence number being indicative of the first trusted time provided on the portable device, the second sequence number being indicative of the second trusted time provided on the further portable device,

if the second trusted time is newer than the first trusted time, performs a verification using the first and second keys, and sets the first sequence number to have a value of the second sequence number if the verification succeeds; and conversely,

if the first trusted time is newer than the second trusted time, performs a verification using the first and second keys, and sets the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device[*See e.g., specification, page 18, lines 19-26*]..

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The rejection of claims 1-44 and 46-58 under 35 U.S.C. § 102(b) as being anticipated by Ishiguro et al. U.S. Patent No. 5,502,765 ("Ishiguro").

VII. ARGUMENT

A. The 35 U.S.C. § 112 First Paragraph Rejection Of Claims 1-58 Should Be Reversed.

The Final Office Action mistakenly states that there is no support for the claimed limitation "so that the older trusted time information embedded on [either] one of the two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device". (See Office Action dated February 22, 2007, page 3).

In the previous Reply, Appellants have noted support for the claimed limitation at specification page 18 lines 26. In particular, the cited portion of the specification reads:

"If the second sequence numbers of the first and second cards 300, 350 are not equal, in step 420, it is determined (by the first card 300 and/or the second card 350) if the second sequence number SEQ2b of the second card 350 is older than the second sequence number SEQ1b of the first card 300, i.e., the time of the second card 350 is older than the time of the first card 300. If so, the [OLDER] second sequence number SEQ2b of the second card 350 is set to have the [NEWER] value of the second sequence number SEQ1b of the first card 300 (step 430). Otherwise, [i.e. conversely, if the second sequence number SEQ2b of the second card 350 is newer than the second sequence number SEQ1b of the first card 300] the [OLDER] second sequence number SEQ1b of the first card 300 is set to have the value of the [NEWER] second sequence number SEQ2b of the second card 350 (step 440)."

(underlining and parenthetical comments added for emphasis). (See also specification FIG. 4)

Appellants submit that this portion of the text is readily understood by a person

skilled in the art as an exchange or replacement of the older time on either card with the newer time on the other card. At least this portion of the specification provides explicit written support for the claimed limitation "so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device."

B. The 35 U.S.C. § 102(b) Rejections Based On Ishiguro Should Be Reversed

The Final Office Action rejects claims 1-44 and 46-58 under 35 U.S.C. § 102(b) as being anticipated by Ishiguro. The anticipation rejection is incorrect and should be reversed.

1. Relevant Case Law

To establish an anticipation rejection, the cited reference must teach every element of the claimed invention. 35 U.S.C. § 102(b) states, in pertinent part, that "[a] person shall be entitled to a patent unless "the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States." A patent claim is anticipated under Section 102 if, among other things, "identity of invention" is shown. *Minnesota Mining and Manufacturing Co. v. Johnson & Johnson Orthopedics, Inc.*, 976 F.2d 1559, 1565, 24 U.S.P.Q.2d 1321 (Fed. Cir. 1985). In finding identity of invention, one "must show that each element of the claim in issue is found . . . in a single prior art reference." *Id.* The Federal Circuit has held that, "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051 (Fed. Cir. 1987). Moreover, "[a] prior

art publication cannot be modified by the knowledge of those skilled in the art for purposes of anticipation." *In re Saunders*, F.2d 599, 602-03, 170 U.S.P.Q. 213, 444 (C.C.P.A. 1971). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim. *In re Bond,* 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

2. Ishiguro Does Not Disclose "If The Second [First] Sequence Number Is Newer . . . Setting The First [Second] Sequence Number To Have A Value Of The Second [First] Sequence Number . . . So That The Older Trusted Time Information Embedded On One Of Two Portable Devices Is Mutually Replaced With The Newer Trusted Time Information Embedded On The Other Portable Device"

Applicants' claim 1 relates to a method for communicating between a first and a second portable devices. The first and second portable devices have embedded thereon first and second sequence numbers comprising information on a first and a second trusted time, respectively. The method of claim 1 includes the steps of:

comparing the first sequence number to the second sequence number including comparing the embedded first and second trusted times;

. . .;

if the second sequence number is newer . . . *setting the first sequence number to have a value of the second sequence number* . . .; and conversely,

if the first sequence number is newer . . . setting the second sequence number to have a value of the first sequence number . . .

so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

Ishiguro does not describe or teach any such two-way mutual updating of the older time with the newer time information.

The Final Office Action mistakenly cites Ishiguro col. 16 line 11 to col. 17 line 16 as describing the combination of the "if-then" steps of claim 1. (See Office Action page 4 last line, page 5 lines 6). Appellants note that careful reading of the cited portion does reveal any teaching of "if the second sequence number is newer . . . *setting the first sequence number to have a value of the second sequence number* . . .; and conversely,

if the first sequence number is newer . . . setting the second sequence number to have a value of the first sequence number . . .".

Appellants submit that any teaching of updating time in Ishiguro is at most one-way (i.e., host to device). Ishiguro does not show or teach the two-way mutual updating of trusted information between two portable devices as described in claim 1.

Further, the Final Office Action page 2 § 4 mistakenly asserts that to Ishiguro col. 15 lines 16-53 teaches "so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device." Appellants note that the cited portion at most teaches " the time stamp . . . set in respective IC card terminal 2 is independently updated." There is no teaching of "mutual" updating between two portable devices.

Thus, Ishiguro does not show or teach the pair of "if-then" elements and the "so that' element of claim 1. For at least this reason, Ishiguro does not anticipate claim 1. Therefore, the rejection of claim 1 (and dependent claims) under 35 U.S.C. § 102(b) should be reversed.

Appellants' claims 25, 32, 37, 41, and 54 include the same or similar "if-then" and so that" limitations of claim 1 discussed above. The arguments relating to claim 1, set out above, are equally applicable to claims 25, 32, 37, 41, and 54, and thus the rejection of claims

25, 32, 37, 41, and 54 (and their dependent claims) under 35 U.S.C. § 102 should likewise be reversed.

VIII. CLAIMS APPENDIX

The rejection of the following claims is appealed.

1. A method for communicating between a first portable device having a first storage device and a second portable device having a second storage device, the first storage device storing thereon a first sequence number and a first key, the second storage device storing thereon a second trusted time and a second key, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices, the method comprising the steps of:

comparing the first sequence number to the second sequence number including comparing the embedded first and second trusted times;

performing a verification using the first and second keys;

if the second sequence number is newer than the first sequence number by comparison of the respective embedded first and second trusted times, setting the first sequence number to have a value of the second sequence number if the verification succeeds; and conversely,

if the first sequence number is newer than the second sequence number by comparison of the respective embedded first and second trusted times, setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

2. The method according to claim 1, wherein the first key is a first global signing key, and the second key is a second global signing key, and wherein the verification is performed by comparing at least one first portion of the first global signing key to at least one second portion of the second global signing key.

3. The method according to claim 2, wherein the verification succeeds when the at least one first portion corresponds to the at least one second portion.

4. The method according to claim 2, wherein each of the first and second global signing keys includes a private key and a public key, and wherein the verification is performed using the respective public keys.

5. The method according to claim 1, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

after the setting step, performing a transaction between the first card and the second card.

6. The method according to claim 1, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

if the verification fails, suspending a transaction between the first card and the second card.

7. The method according to claim 1, further comprising the step of:

if the verification fails, recording a failure of the verification in at least one of the first storage device and the second storage device.

8. The method according to claim 1, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

if the first sequence number and the second sequence number are equal, performing a transaction between the first card and the second card.

9. The method according to claim 1, wherein the first portable device is a first card, and the second portable device is a second card, wherein the setting step is performed by transmitting an authenticated system message ("ASM") command from the second card to the first card, and wherein at least one of the first and second cards sets the second sequence number.

10. The method according to claim 1, wherein the first portable device is a first card, and the second portable device is a second card, and wherein the first storage device stores a third sequence number thereon, wherein the second storage device stores a fourth sequence number thereon, and further comprising the steps of:

if the first sequence number and the second sequence number are equal, determining whether the third sequence number corresponds to the fourth sequence number; and

if the third sequence number does not correspond to the fourth sequence number, transmitting an authenticated system message ("ASM") command from a particular card of the first and second cards having a newer number of the third and fourth sequence numbers to another card of the first and second cards.

11. The method according to claim 10, wherein the ASM command is transmitted without setting the first sequence number to have the value of the second sequence number.

12. The method according to claim 10, further comprising the step of:

if the third sequence number corresponds to the fourth sequence number, performing a transaction between the first card and the second card.

13. The method according to claim 1, wherein the first key is a first global signing key, and the second key is a second global signing key, and wherein the first global signing key relates to the first sequence number, and the second global signing key relates to the second sequence number.

14. The method according to claim 1, wherein the first key is a first global signing key, and the second key is a second global signing key, and wherein the first global signing key is associated with a first value transfer protocol ("VTP") key, and the second global signing key is associated with a second VTP key, the first VTP key being stored in the first storage device, the second VTP key being stored in the second storage device.

15. The method according to claim 1, wherein each of the first portable device and the second portable device includes a processing device.

16. The method according to claim 1, further comprising the steps of:

receiving an authenticated system message which includes a command; and

executing the command.

17. The method according to claim 1, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

providing an application to at least one card of the first and second cards, the application is provided for at least one of:

renewing a security feature of the at least one card, and

updating a security scheme of the at least one card on-chip risk management.

18. The method according to claim 1, further comprising the step of:

providing a reference point for time to at least one of the first and second portable devices from a central command arrangement.

19. The method according to the claim 1, further comprising the steps of:

enabling a selective targeting of at least one device of the first and second portable devices; and

applying re-customization procedures on the at least one device.

20. The method according to the claim 19, further comprising the step of:

selecting a particular response by the at least one device when a predetermined criteria is met.

21. The method according to claim 1, wherein the first key is a first global signing key, and the second key is a second global signing key, and wherein the verification is performed by

comparing cryptograms which are related to the first global signing key and the second global signing key.

22. The method according to claim 20, further comprising the steps of:

generating the cryptograms by one of the first portable device and the second portable device; and

verifying the cryptograms using another one of the first portable device and the second portable device.

23. The method according to claim 20, wherein the cryptograms are generated by a central authority.

24. The method according to claim 1, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

after the setting step, modifying stored parameters of at least one of the first and second cards to at least one of suspend, permit and modify subsequent operations between the first and second cards or other cards.

25. A portable device which is capable of performing a transaction with a further portable device, comprising:

a storage device storing a first sequence number and a first key wherein the first sequence number comprises information on a first trusted time embedded in the storage device; and

a processing device performing the following steps:

receiving a second sequence number and a second key from the further portable device, wherein the second sequence number comprises information on a second trusted time embedded in the further portable device,

comparing the first sequence number to the second sequence number including comparing the embedded first and second trusted times;

performing a verification using the first and second keys;

if the second sequence number is newer than the first sequence number by comparison of the respective embedded first and second trusted times, setting the first sequence number to have a value of the second sequence number if the verification succeeds; and conversely,

if the first sequence number is newer than the second sequence number by comparison of the respective embedded first and second trusted times, setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

26. The portable device according to claim 25, wherein, if the verification fails, the processing device suspends the transaction with the further portable device, and records a failure of the verification.

27. The portable device according to claim 25, wherein, if the first sequence number and the second sequence number are equal, the processing device performs the transaction with the further portable device.

28. The portable device according to claim 25, wherein the storage device stores a third sequence number thereon, and wherein the processing device performs the following:

if the first sequence number and the second sequence number are equal, and determines whether the third sequence number corresponds to a fourth sequence number of the further portable device.

29. The portable device according to claim 28, wherein, if the third sequence number corresponds to the fourth sequence number, the processing device performs the transaction with the further portable device.

30. The portable device according to claim 25, wherein the portable device is a smart card, and wherein the further portable device is a further smart card.

31. The portable device according to claim 25, wherein the first key is a global signing key, and wherein the second key is a second global signing key.

32. A method for determining an approximate current time using a first portable device and a second portable device, the first portable device having a first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number, the second storage device storing thereon a second sequence number, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices, the method comprising the steps of:

comparing the first sequence number to the second sequence number, the first sequence number being indicative of ~~a~~ the first trusted time provided on the first portable device, the second sequence number being indicative of ~~a~~ the second trusted time provided on the second portable device; and

if the first trusted time is older than the second trusted time, setting the first sequence number to have a value of the second sequence number and conversely,

if the second trusted time is older than the first trusted time, setting the second sequence number to have a value of the first sequence number so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

33. The method according to claim 32, further comprising the step of:

if the second time is older than the first time, setting the second sequence number to have a value of the first sequence number.

34. The method according to claim 33, further comprising the step of:

after the setting step and if the first time is not equal to the second time, executing an action which is triggered by at least one of the first sequence number and the second sequence number.

35. The method according to claim 34, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

after the executing step and if the first time is not equal to the second time, performing a transaction between the first card and the second card.

36. The method according to claim 32, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

if the first time is equal to the second time, performing a transaction between the first card and the second card.

37. A portable device which is capable of determining an approximate current time during a communication with a further portable device, comprising:

a storage device storing a first sequence number wherein the first sequence number comprises information on a first trusted time embedded in the storage device; and

a processing device performing the following:

receives a second sequence number from the further portable device number wherein the second sequence number comprises information on a second trusted time embedded in the further portable device,

compares the first sequence number to the second sequence number, the first sequence number being indicative of ~~a~~ the first trusted time provided on the portable device, the second sequence number being indicative of ~~a~~ the second trusted time provided on the further portable device, and

executes one of the following actions:

if the first trusted time is older than the second trusted time, sets the first sequence number to have a value of the second sequence number; and conversely,

if the second trusted time is older than the first trusted time, sets the second sequence number to have a value of the first sequence number so that the older trusted time information embedded on one of two portable

devices is mutually replaced with the newer trusted time information embedded on the other portable device.

38. The portable device according to claim 37, wherein, if the first time is not equal to the second time, the processing device executes a particular action which is triggered by at least one of the first sequence number and the second sequence number.

39. The portable device according to claim 37,

wherein the portable device is a smart card, and the further portable device is a further smart card, and

wherein, after the execution of the particular action and if the first time is not equal to the second time, the processing device performs a transaction between the smart card and the further smart card.

40. The portable device according to claim 37,

wherein the portable device is a smart card, and the further portable device is a further smart card, and

wherein, if the first time is equal to the second time, the processing device performs a transaction between the smart card and the further smart card.

41. A method for determining an approximate current time using a first portable device and a second portable device, the first portable device having a first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number and a first key, the second storage device storing thereon a second sequence number and a second key, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices, the method comprising the steps of:

comparing the first sequence number to the second sequence number, the first sequence number being indicative of a the first trusted time provided on the first portable device,

the second sequence number being indicative of ~~a~~ the second trusted time provided on the second portable device;

if the second trusted time is newer than the first trusted time, performing a verification using at least one of the first and second keys; and

setting the first sequence number to have a value of the second sequence number if the verification succeeds; and conversely,

if the first trusted time is newer than the second trusted time, performing a verification using at least one of the first and second keys; and

setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

42. The method according to claim 41, further comprising the steps of:

generating the cryptograms by one of the first portable device and the second portable device; and

verifying the cryptograms using another one of the first portable device and the second portable device.

43. The method according to claim 41, wherein the first key is a first global signing key, and the second key is a global signing key, and wherein the verification is performed by comparing at least one first portion of the first global signing key to at least one second portion of the second global signing key.

44. The method according to claim 43, wherein the verification succeeds when the at least one first portion corresponds to the at least one second portion.

45. The method according to claim 43, wherein each of the first and second global signing keys includes a private key and a public key, and wherein the verification is performed using the respective public keys.

46. The method according to claim 41, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

after the setting step, performing a transaction between the first card and the second card.

47. The method according to claim 41, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

if the verification fails, suspending a transaction between the first card and the second card.

48. The method according to claim 41, further comprising the step of:

if the verification fails, recording a failure of the verification in at least one of the first storage device and the second storage device.

49. The method according to claim 41, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

if the first time and the second time are equal, performing a transaction between the first card and the second card.

50. The method according to claim 41,

wherein the first portable device is a first card and the second portable device is a second card,

wherein the setting step is performed by transmitting an authenticated system message command from the second card to the first card, and

wherein at least one of the first and second cards sets the second sequence number.

51. The method according to claim 41, wherein the first key is a first global signing key, and the second key is a global signing key, and wherein the first global signing key relates to the first sequence number, and the second global signing key relates to the second sequence number.

52. The method according to claim 41, wherein the first key is a first global signing key, and the second key is a global signing key, and wherein the first global signing key is associated with a first value transfer protocol ("VTP") key, and the second global signing key is associated with a second VTP key, the first VTP key being stored in the first storage device, the second VTP key being stored in the second storage device.

53. The method according to claim 41, wherein each of the first portable device and the second portable device includes a processing device.

54. A portable device which is capable of determining an approximate current time during a communication with a further portable device, comprising:

a storage device storing a first sequence number and a first key wherein the first sequence number comprises information on a first trusted time embedded in the storage device; and

a processing device performing the following:

receives a second sequence number and a second key from the further portable device wherein the second sequence number comprises information on a second trusted time embedded in the further portable device,

compares the first sequence number to the second sequence number, the first sequence number being indicative of the first trusted time provided on the portable device, the second sequence number being indicative of the second trusted time provided on the further portable device,

if the second trusted time is newer than the first trusted time, performs a verification using the first and second keys, and sets the first sequence number to have a value of the second sequence number if the verification succeeds; and

conversely,

if the first trusted time is newer than the second trusted time, performs a verification using the first and second keys, and sets the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

55. The portable device according to claim 54, wherein, if the verification fails, the processing device suspends the transaction with the further portable device, and records a failure of the verification.

56. The portable device according to claim 54, wherein, if the first sequence number and the second sequence number are equal, the processing device performs the transaction with the further portable device.

57. The portable device according to claim 54, wherein the portable device is a smart card, and wherein the further portable device is a further smart card.

58. The portable device according to claim 54, wherein the first key is a first global signing key and the second key is a second global signing key.

IX. EVIDENCE APPENDIX

None.

X, RELATED PROCEEDINGS APPENDIX

None.

For the foregoing reasons, the Examiner' rejection of claims 1-58 should be reversed.

Respectfully submitted,

By: _____

Manu J Tejwani
Patent Office Reg. No. 37,952

Telephone: (212) 408-2614

Attorneys for Appellants
Baker Botts L.L.P.
30 Rockefeller Plaza
New York, NY 10112